

# Symbolic Integration in Prime Characteristic

Bill Allombert

## Abstract

In this paper we study elementary extensions of differential fields in prime characteristic. In particular, we show that, in contrast to Liouville's result in characteristic zero, all elements of an elementary extension admit an antiderivative in some logarithmic extension.

## 1 Introduction

### 1.1 Motivation

In a famous paper [L], Liouville proved that some elementary functions of a real or complex variable do not admit elementary antiderivatives, the usual example being  $x \mapsto \exp(x^2)$ . In 1968, Risch gave an algorithm ([Ri]) to decide if an elementary function of a real or complex variable admits an elementary antiderivative.

The modern definition of elementary functions [Ro] as elements of an elementary differential extension of  $\mathbb{C}(X)$  can be generalised to any base field. In this paper, we study the problem when the base field has finite characteristic.

In this paper we study differential fields in prime characteristic from the point of view of symbolic integration. Below is an example of the kind of phenomenon which interests us.

Let  $K = \mathbb{F}_p(X, E)$  and  $\partial$  the derivation defined by  $\partial(X) = 1$  and  $\partial(E) = 2XE$ . The element  $E$  satisfies the same first-order linear differential equation than the complex function  $f : x \mapsto \exp(x^2)$ , namely  $f' = 2xf$ , thus we can see  $E$  as a  $\mathbb{F}_p$ -analogue of  $f$ . However if we pick  $p = 3$  and set  $y = \frac{1-X^2}{X^3}E$ , or pick  $p = 5$  and set  $y = \frac{X^4-2X^2+2}{2X^5}E$ , a straightforward computation shows that in both case  $\partial(y) = E$ , while  $f$  is known not to have an antiderivative.

The object of this paper is to study whether such formulae always exist and how to compute them.

We will make use of iterated derivations in the naive sense, and not use Hasse derivatives, even though we are in finite characteristic. However the more striking results we obtain can be stated without reference to iterated derivations, but they will play a crucial role in the proofs.

## 2 Definitions

Let  $K$  be a field. A *derivation* on  $K$  is a group homomorphism  $\partial = \partial_K$  from  $K$  to  $K$  such that for all  $a, b$  in  $K$  the following holds:

$$\partial(ab) = \partial(a)b + a\partial(b) .$$

The kernel of  $\partial_K$  is a field called the field of constants of  $(K, \partial_K)$ , and is denoted by  $C(K)$ .

A pair  $(K, \partial_K)$  is a *differential field* if  $K$  is a field and  $\partial_K$  is a derivation on  $K$ .

A *differential extension* of  $(K, \partial_K)$  is a differential field  $(L, \partial_L)$  such that  $L/K$  is a field extension and  $\partial_L|_K = \partial_K$ .

Let  $p$  be a prime number and  $(K, \partial_K)$  be a differential field of characteristic  $p$ . Derivations in characteristic  $p$  have two specific properties:

- for all  $a \in K$ ,  $\partial(a^p) = 0$ .
- for all positive integers  $e$ ,  $\partial^{p^e}$  is a derivation.

The simplest non-trivial example of a differential field in characteristic  $p$  is  $(\mathbb{F}_p(X), \partial)$  where  $\partial(F) = F'$ .

Furthermore the  $p$ -th derivative of an element of  $\mathbb{F}_p[X]$  is zero. As a consequence,  $X^{p-1}$  does not admit a polynomial antiderivative: indeed, by Wilson's formula we have  $\partial^{p-1}(X^{p-1}) = -1$ , so if  $u$  was a polynomial antiderivative of  $X^{p-1}$  we would have  $\partial^p(u) = -1$ , a contradiction.

A second issue is that inseparable algebraic extensions either cannot be provided with a compatible derivation, or admit an infinite number of compatible derivations. Consider the fields  $K = \mathbb{F}_p(X)$  and  $L = \mathbb{F}_p(X^{1/p})$  (for the usual derivation).

The identity  $\partial_L(X) = \partial((X^{1/p})^p) = 0$  is incompatible with  $\partial_K(X) = 1$ . It follows that  $L/K$  is an algebraic extension of fields which cannot be extended to an extension of differential fields.

A third issue is that if  $L/K$  is a transcendental extension of differential fields, then  $C(L)$  will be a transcendental extension of  $C(K)$ .

Thus, by contrast to characteristic 0, it is not possible to require that  $C(L) = C(K)$ . Instead, we could require that  $C(L) = L^p C(K)$ , but we will not need it.

## 2.1 Elementary extensions

**Definition 1** A differential extension  $(L, \partial_L)$  of  $(K, \partial_K)$  is logarithmic of type “ $\log(u)$ ” if there exists  $u \in K$  and  $y \in L$  generating  $L$  over  $K$  such that  $\partial(u) = \partial(y)u$ .

**Definition 2** A differential extension  $(L, \partial_L)$  of  $(K, \partial_K)$  is exponential of type “ $\exp(u)$ ” if there exists  $u \in K$  and  $y \in L$  generating  $L$  over  $K$  such that  $\partial(y) = \partial(u)y$ .

**Definition 3** A differential extension  $(L, \partial_L)$  of  $(K, \partial_K)$  is elementary if there exists a tower of differential extensions  $L_0 = K \subseteq L_1 \dots \subseteq L_n = L$  such that each extension  $L_{i+1}/L_i$  is either algebraic separable, logarithmic, or exponential.

## 2.2 Linear differential operators

This section lists some basic results about linear differential operators in characteristic  $p$  that will be useful.

Let  $(K, \partial_K)$  be a differential field. The map  $\partial_K$  is an endomorphism of the  $C(K)$ -vector space  $K$ . If  $P$  is a polynomial with coefficients in  $C(K)$ , we denote by  $P(\partial_K)$  the application of  $P$  to  $\partial_K$  in the algebra of  $C(K)$ -endomorphisms of  $K$ .

Let  $y$  be an element of  $K$ . The annihilator of  $y$ ,  $\text{Ann}(y) = \{P \in C(K)[X] \mid P(\partial)(y) = 0\}$ , is an ideal of the polynomial ring  $C(K)[X]$ .

The element  $y \in K$  satisfies a linear differential equation with constant coefficients if and only if  $\text{Ann}(y) \neq \{0\}$ .

**Definition 4 ( $p$ -polynomials)** (See [J, page 234].) A polynomial  $P$  over a field  $K$  is a  $p$ -polynomial if it can be written as  $P = \sum_{j=0}^n a_j X^{p^j}$  with  $a_j \in K$  for  $0 \leq j \leq n$ .

**Lemma 1** If  $K$  is a field and  $I$  a non-zero ideal of  $K[X]$ , then  $I$  contains a non zero  $p$ -polynomial.

Since  $I$  is non-zero, the quotient  $K[X]/I$  is a finite dimensional  $K$ -vector space. If  $\pi$  denotes the projection from  $K[X]$  to  $K[X]/I$ , it follows that the infinite family  $(\pi(X^{p^n}))_{n \geq 0}$  is  $K$ -linearly dependent. Thus there exist elements  $(a_j)_{j=1}^k$  of  $K$ , not all zero, such that  $\sum_{j=1}^k a_j \times X^{p^j} \in I$ .

**Lemma 2** *Let  $(K, \partial_K)$  be a differential field, and  $(y_i)_{i=1}^n$  be a family of elements of  $K$ . If the  $y_i$  satisfy a linear differential equation with constant coefficients for all  $1 \leq i \leq n$ , then there exists a non-zero  $p$ -polynomial  $P$  in  $C(K)[X]$  such that  $P(\partial)(y_i) = 0$  for all  $1 \leq i \leq n$ .*

Let  $I = \bigcap_{i=1}^n \text{Ann}(y_i)$ . Since  $\text{Ann}(y_i) \neq \{0\}$  for all  $1 \leq i \leq n$  and  $C(K)[X]$  is a domain,  $I \neq \{0\}$ . From the lemma, it follows that there exists a non-zero  $p$ -polynomial  $P$  in  $C(K)$  such that  $P \in I$ , so in particular  $P(y_i) = 0$  for all  $1 \leq i \leq n$ .

**Proposition 1** *If  $(K, \partial)$  is a differential field of characteristic  $p > 0$  and  $P$  is a  $p$ -polynomial in  $C(K)$ , then the  $C(K)$ -endomorphism  $P(\partial)$  is a derivation which commutes with  $\partial$ .*

This follows from the fact that for all  $j \geq 1$ ,  $\partial^{p^j}$  is a derivation.

We will make use of the following notation.

**Lemma 3** *Let  $(K, \partial)$  be a differential field and  $Q = \sum_{i=0}^n a_i X^i \in K[X]$  be a polynomial. We set*

$$Q^\partial = \sum_{i=0}^n \partial_K(a_i) X^i .$$

If  $u \in K$  then

$$\partial(Q(u)) = \partial(u)Q'(u) + Q^\partial(u) .$$

### 3 Linear differential fields

#### 3.1 Linear fields

**Definition 5** *Let  $(K, \partial_K)$  be a differential field, let  $y$  be an element of  $K$ , and let  $C$  be a sub-differential field of  $K$ . We will say that  $y \in K$  satisfies a linear differential equation with coefficients in  $C$  if there exists a non-zero polynomial  $P \in C[X]$  such that  $P(\partial)(y) = 0$ .*

**Definition 6** *A differential field  $(K, \partial_K)$  is linear if every element satisfies a linear differential equation with coefficients in  $C(K)$ .*

#### 3.2 Linear extensions

This section establishes that some common type of extensions of linear differential fields are linear.

**Proposition 2** *Let  $(K, \partial_K)$  be a differential field. The set  $F$  of elements of  $K$  that satisfy a linear differential equation with coefficients in  $C(K)$  is a sub-differential field of  $K$ .*



Let  $u$  and  $v$  be two elements of  $F$ . By Lemma 2, there exists a  $p$ -polynomial  $P \in C(K)[X]$  such that  $P(\partial)(u) = 0$  and  $P(\partial)(v) = 0$ . Since  $P(\partial)$  is a derivation,  $\ker P(\partial)$  is a field, so  $P(\partial)(u+v) = 0$ ,  $P(\partial)(uv) = 0$ , and if  $u \neq 0$ ,  $P(\partial)(u^{-1}) = 0$  and  $P(\partial)(\partial(u)) = \partial(P(\partial)(u)) = 0$ .



We conclude that  $F$  is a differential field.

**Lemma 4** *Let  $(K, \partial_K)$  be a linear differential field, and let  $(L, \partial_L)$  be a differential extension of  $(K, \partial_K)$ . If  $L/K$  is algebraic separable, then  $(L, \partial_L)$  is linear.*




Let  $y$  be an element of  $L$  and  $U = \sum_{i=0}^n u_i X^i$  be its minimal polynomial over  $K$ . By Lemma 2, there exists a non-zero  $p$ -polynomial  $P$  in  $C(K)[X]$  such that  $P(\partial)(u_i) = 0$  for all  $0 \leq i \leq n$ . Since  $P(\partial)$  is a derivation,

$$\sum_{i=0}^n P(\partial)(u_i y^i) = \sum_{i=0}^n P(\partial)(u_i) y^i + \sum_{i=0}^n u_i i P(\partial)(y) y^{i-1} ,$$

so

$$\sum_{i=0}^n P(\partial)(u_i y^i) = P(\partial)(y) U'(y) .$$

Since  $U(y) = 0$ , it follows that  $\sum_{i=0}^n P(\partial)(u_i y^i) = 0$ , and so  $P(\partial)(y) U'(y) = 0$ . Since  $y$  is separable,  $U'(y) \neq 0$ , so  $P(\partial)(y) = 0$ . 

**Lemma 5** *Let  $(K, \partial_K)$  be a linear differential field, and let  $(L, \partial_L)$  be a differential extension of  $(K, \partial_K)$ . If  $L/K$  is of exponential type then  $(L, \partial_L)$  is linear.*



The field  $L$  is generated by an element  $y$  such that there exists  $u \in K$  with  $\partial(y) = \partial(u)/u$ , or equivalently  $u\partial(y) = \partial(u)$ . This is a classical differential equation, whose derivatives are given by the multivariate Bell polynomials. In particular in characteristic  $p$ , Carlitz [C] Formula (1.4) gives the equation

$$\partial^{p^r}(y) = \left( \sum_{i=0}^r \partial^{p^i}(u)^{p^{r-i}} \right) y . \quad (1)$$

We note that

$$c_r = \sum_{i=0}^{r-1} \partial^{p^i}(u)^{p^{r-i}}$$


belongs to  $C(K)$ , and we rewrite the equation as

$$\partial^{p^r}(y) = (\partial^{p^r}(u) + c_r) y .$$


By Lemma 2, there exists a family  $(a_j)_{j=1}^k$  of elements of  $C(K)$  not all equal to 0 such that  $\sum_{j=0}^k a_j \partial^{p^j}(u) = 0$ . It follows that

$$\sum_{j=0}^k a_j \partial^{p^j}(y) = \left( \sum_{j=0}^k a_j \partial^{p^j}(u) \right) y + \left( \sum_{j=0}^k a_j c_j \right) y \quad (2)$$

$$= \left( \sum_{j=0}^k a_j c_j \right) y . \quad (3)$$

Since the  $a_j$  are not all equal to 0 and  $\sum_{j=0}^k a_j c_j$  belongs to  $C(K)$ ,  $y$  satisfies a linear differential equation with coefficients in  $C(K)$ , so by Theorem 4  $L$  is linear. 

**Lemma 6** *Let  $(K, \partial_K)$  be a linear differential field, and let  $(L, \partial_L)$  be a differential extension of  $(K, \partial_K)$ . If  $L/K$  is of logarithmic type then  $(L, \partial_L)$  is linear.*

 There exists a generator  $y$  of  $L$  and  $u \in K$  such that  $\partial(y) = \partial(u)/u$ , or equivalently  $u\partial(y) = \partial(u)$ . By applying Carlitz's formula, we have

$$\partial^{p^r}(u) = \left( \sum_{i=0}^r (\partial^{p^i}(y))^{p^{r-i}} \right) u . \quad (4)$$

We note that  $c_r = \sum_{i=0}^{r-1} (\partial^{p^i}(y))^{p^{r-i}}$  belongs to  $C(L)$  and we rewrite the equation as  $\partial^{p^r}(u) = (\partial^{p^r}(y) + c_r)u$ . By Lemma 2, there exists a family  $(a_j)_{j=1}^k$  of elements of  $C(K)$  not all equal to 0 such that


$$\sum_{j=0}^k a_j \partial^{p^j}(u) = 0 .$$

From

$$\sum_{j=0}^k a_j \partial^{p^j}(u) = \left( \sum_{j=0}^k a_j \partial^{p^j}(y) + \sum_{j=0}^k a_j c_j \right) u \quad (5)$$

it follows that

$$\sum_{j=0}^k a_j \partial^{p^j}(y) + \sum_{j=0}^k a_j c_j = 0 ,$$

and since  $\sum_{j=0}^k a_j c_j$  belongs to  $C(L)$ ,  $\sum_{j=1}^k a_j \partial^{p^j+1}(y) = 0$ . Since the  $a_j$  are not all equal to 0,  $y$  satisfies a linear differential equation with coefficients in  $C(K)$ , so by Theorem 4  $L$  is linear. 

We have thus proved:

**Theorem 1** *Let  $(K, \partial_K)$  be a linear differential field, and let  $(L, \partial_L)$  be a differential extension of  $(K, \partial_K)$ . If  $L/K$  is elementary, then  $(L, \partial_L)$  is linear.*

The following is a generalization of Lemma 5.

**Theorem 2** *Let  $(K, \partial_K)$  be a linear differential field, and  $(L, \partial_L)$  a differential extension of  $(K, \partial_K)$ . If  $y \in L$  satisfies a linear differential with coefficients in  $K$  then it satisfies a linear differential equation with coefficients in  $C(K)$ .*


 Let  $u_0, \dots, u_n$  in  $K$  with  $u_n \neq 0$  be such that

$$u_0 y + u_1 \partial_L(y) + u_2 \partial_L(\partial_L(y)) \dots + u_n \partial_L^n(y) = 0 .$$

By Lemma 2, there exists a non-zero  $p$ -polynomial  $P \in C(K)[X]$  such that  $P(\partial_K)(u_i) = 0$  for all  $0 \leq i \leq n$ . Since  $P(\partial_K)$  is a derivation, the  $C(K)$  vector space  $F = \ker P(\partial_K)$  is a subfield of  $K$  that contains  $(u_i)_{i=0}^n$  and with constant field  $C(F) = C(K)$ .

Let  $E$  be the sub- $F$ -vector space of  $L$  spanned by  $(\partial^k(y))_{k=0}^{n-1}$ . It follows from the differential equation that  $E$  is stable by  $\partial_L$ , and the restriction  $D$  of  $P(\partial_L)$  to  $E$  is an  $F$ -endomorphism of  $E$ . Let  $Q \in F[X]$  be the monic minimal polynomial of  $D$ . If  $v \in E$  then  $Q(D)(v) = 0$ , and so  $\partial_L(Q(D)(v)) = 0$ . Since  $\partial$  and  $D$  commute,

$$\partial_L(Q(D)(v)) = Q^\partial(D)(v) + Q(D)(\partial_L(v)) .$$

Since  $Q(D) = 0$ , it follows that  $Q^\partial(D)(v) = 0$  for all  $v \in E$ . Since  $Q$  is the minimal polynomial of  $D$  and the degree of  $Q^\partial$  is strictly less than the degree of  $Q$  (since  $Q$  is monic), it follows that  $Q^\partial = 0$ , so  $Q$  belongs to  $C(K)[X]$ . In particular it follows that  $Q(P)$  is a non-zero element of  $C(K)[X]$  which satisfies  $(Q(P))(\partial_L)(y) = 0$ . 

**Example 1** Let  $K = (\mathbb{F}_3(X), \partial_K)$  be such that  $\partial_K(X) = 1$ , and let  $L$  be the differential extension  $(\mathbb{F}_3(X, Y, Y_1), \partial_L)$  where  $\partial_L(X) = 1$ ,  $\partial_L(Y) = Y_1$  and  $\partial_L(Y_1) = XY$ .

The element  $Y$  satisfies the linear equation  $\partial^2(Y) = XY$  (the Airy [A] equation) with coefficients in  $F = \mathbb{F}_3(X)$  and  $\partial^3(X) = 0$ . By applying  $\partial$ , it follows that  $\partial^3(Y) = Y + XY_1$  and  $\partial^3 Y_1 = \partial^4(Y) = 2Y_1 + X^2 Y$ . Thus the matrix of  $\partial^3$  in the basis  $(Y, Y_1)$  is  $\begin{pmatrix} 1 & X^2 \\ X & 2 \end{pmatrix}$ , whose minimal polynomial is  $P(T) = T^2 - X^3 - 1$ . Thus  $Y$  satisfies the equation  $\partial^6(Y) = (X^3 + 1)Y$  with coefficients in  $C(F) = \mathbb{F}_3(X^3)$ .

## 4 Integration

**Lemma 7** Let  $(K, \partial)$  be a differential field of characteristic  $p > 0$ . If  $u \in K$  is such that  $\partial^{p^k}(u) \in C(K)^\times$  and  $y \in K$  is such that  $\partial(y) = \partial(u)/u$ , then  $\partial^{p^{k+1}}(y) \in C(K)^\times$ .




By applying again Carlitz's formula to the identity  $\partial(u) = \partial(y)u$ , we obtain

$$\partial^{p^k}(u) = \left( \sum_{i=0}^k \partial^{p^i}(y) u^{p^{k-i}} \right) u . \quad (6)$$

After setting  $D = \partial^{p^k}$  and  $c_k = \sum_{i=0}^{k-1} \partial^{p^i}(y) u^{p^{k-i}} \in C(K)$ , the equation reads

$$D(u)/u = D(y) + c_k . \quad (7)$$

Since the endomorphism  $D$  is a derivation of  $K$  whose kernel contains  $C(K)$ , if  $F$  is a polynomial with coefficients in  $C(K)$  then  $D(F(u)) = D(u)F'(u)$ . Since the  $p-1$ -st derivative of the polynomial  $X^{p-1}$  is equal to  $-1$  by Wilson's theorem, we obtain the formula:  $D^{p-1}(u^{p-1}) = -D(u)u^{p-1}$ . Noting that  $D^{p-1} = \partial^{p^{k+1}-p^k}$ , it follows that  $-D(u)^p/u^p = \partial^{p^{k+1}}(y)$ , and since  $D(u) \in C(K)^\times$  we have proved that  $\partial^{p^{k+1}}(y) \in C(K)^\times$ . 

**Proposition 3** Let  $(K, \partial)$  be a differential field of characteristic  $p > 0$ ,  $n \geq 0$  an integer, and  $u \in K$  such that  $\partial^{p^n}(u) = 1$ . There exists a logarithmic extension  $L/K$  of type  $\log(u)$  and  $y \in L$  such that  $\partial^{p^{n+1}}(y) = 1$ .

☺ We denote by  $L$  the field of rational functions  $K(z)$ . We extend the derivation  $\partial_K$  to  $L$  by setting  $\partial(z) = \partial(u)/u$ . The extension  $L/K$  is logarithmic of type  $\log(u)$ . It follows from the lemma that  $c = \partial^{p^{k+1}}(z) \in C(L)^\times$ , so by setting  $y = z/c$ , it follows that  $\partial^{p^{k+1}}(z/c) = 1$ . ☺

It is possible to prove a more precise result:

**Proposition 4** *Let  $(K, \partial)$  be a differential field of characteristic  $p > 0$ ,  $n \geq 0$  an integer, and  $u \in K$  such that  $\partial^n(u) = 1$ . Then either there exists  $y \in K$  such that  $\partial^{p^{n+1}}(y) = 1$ , or there exists a differential extension  $L/K$  of logarithmic type such that  $C(L) = C(K)L^p$  and  $y \in L$  such that  $\partial^{p^{n+1}}(y) = 1$ .*

☺ We assume that the equation  $\partial^{p^{n+1}}(y) = 1$  has no solution  $y \in K$ . By the lemma, this implies that the equation  $\partial(z) = \partial(u)/u$  has no solution  $z \in K$ . We build  $L = K(z)$  as in Proposition 3. It only remains to prove that  $C(L) = C(K)L^p$ . An element of  $C(L)$  can be written as  $f(z)/g(z)$  where  $f$  and  $g$  are two elements of  $K[X]$ . We set  $Q = fg^{p-1} \in K[X]$ . Since  $f(z)/g(z) = Q(z)/g(z)^p$ , it follows that  $Q \in C(L)$  and that proving  $Q(z) \in C(K)L^p$  will prove that  $f(z)/g(z) \in C(K)L^p$ .

We write  $Q = \sum_{i=0}^m a_i X_i$  with  $a_i \in K$ . Since  $\partial(Q(y)) = 0$ , it follows that

$$\partial(u)Q'(y) + uQ^\partial(y) = 0 .$$

By identifying coefficients we find the equations

$$u\partial(a_m) = 0 \tag{8}$$

$$\partial(u)(i+1)a_{i+1} + u\partial(a_i) = 0 \tag{9}$$

By using the fact that the equation  $\partial(u)c = u\partial(z)$  with unknowns  $c \in C(K)$  and  $z \in K$  only admits the solution  $c = 0, z = 0$ , it follows easily by induction that  $Q \in C(K)[X^p]$ , so  $Q(y) \in C(K)(y^p) = C(K)L^p$ . ☺

**Proposition 5** *Let  $(K, \partial)$  be a differential field of characteristic  $p > 0$ ,  $n$  a positive integer, and  $u \in K$  such that  $\partial^n(u) = 1$ . Then either there exists  $y \in K$  such that  $\partial^{n+1}(y) = 1$ , or there exists a logarithmic extension  $L/K$  such that  $C(L) = C(K)L^p$  and  $y \in L$  such that  $\partial^{n+1}(y) = 1$ .*

☺ Write  $n = p^k + l$  with  $l \geq 0$  and  $k$  as large as possible, and assume that the equation  $\partial^{n+1}(y) = 1$  has no solution in  $K$ . This implies that the equation  $\partial^{p^{k+1}}(y) = 1$  has no solution in  $K$ . By Proposition 4, we build  $L$  satisfying the above conditions and  $z$  such that  $\partial^{p^{k+1}}(z) = 1$ . We set  $y = \partial^{p^{k+1}-(n+1)}(z)$  and it follows that  $\partial^{n+1}(y) = 1$ . ☺

## 5 Antiderivable fields

**Definition 7** *A differential field  $(K, \partial)$  is antiderivable if it is linear and such that  $\partial$  takes the value 1 on  $K$ .*

**Example 2** *The differential field  $(\mathbb{F}_p(X), \partial)$  where  $\partial$  is the standard derivation is antiderivable. Indeed, every element  $u$  satisfies  $\partial^p(u) = 0$ , and  $\partial(X) = 1$ .*

**Proposition 6** *An elementary extension of an antiderivable differential field is antiderivable.*

☺ This follows from Theorem 1 and the fact that if  $\partial$  takes the value 1 over  $K$ , it takes it a fortiori over any larger field. ☺

**Lemma 8** *Let  $(K, \partial)$  be a differential field, and  $u$  and  $v$  be two elements of  $K$ . If there exists an integer  $n \geq 1$  such that  $\partial^n(u) = 0$  and  $\partial^{n-1}(v) = 1$ , then  $u$  belongs to the vector space generated by  $(\partial^k(v))_{k=0}^{n-1}$  over  $C(K)$ .*

☺ This is a classical result. If  $n = 1$ , then  $v = 1$  and  $u \in C(K)$ , so the result is true. Otherwise assume by induction that the result is true for  $n$ . Let  $u$  and  $v$  be such that  $\partial^{n+1}(u) = 0$  and  $\partial^n(v) = 1$ . It follows that  $\partial(u)$  and  $\partial(v)$  satisfy  $\partial^n(\partial(u)) = 0$  and  $\partial^{n-1}(\partial(v)) = 1$ . By the induction hypothesis, there exist elements  $(c_i)_{i=0}^{n-1}$  in  $C(K)$  and not all zero, such that  $\partial(u) = \sum_{k=0}^{n-1} c_k \partial^k(\partial(v)) = 0$ . By setting  $S = \sum_{k=0}^{n-1} c_k \partial^k(v)$ , it follows that  $c_n = u - S$  belongs to  $C(K)$ . Since  $\partial^n(v) = 1$  we have  $u = \sum_{k=0}^n c_k \partial^k(v)$ , which concludes the proof. ☺

The following result justifies the definition:

**Theorem 3** *Let  $(K, \partial)$  be an antiderivable differential field. Every element  $u \in K$  admits an antiderivative in an extension of logarithmic type.*

☺ By hypothesis,  $u$  satisfies a linear differential equation with coefficients in  $C(K)$ . Thus there exist  $n \geq 0$  and  $(a_i)_{i=1}^k$  in  $C(K)$  such that  $\partial^n(u) = \sum_{i=1}^k a_i \partial^{n+i}(u)$ . Set  $v = \sum_{i=1}^k a_i \times \partial^{i-1}(u)$  and  $w = \partial(v) - u$ , so that  $\partial^n(w) = 0$ . If  $n = 0$  then  $v$  is an antiderivative of  $u$ . Otherwise, we may assume that  $n$  is minimal for the given  $(a_i)_{i=1}^k$ , in other words that  $\partial^{n-1}(w) \neq 0$ , and so  $\partial^{n-1}(w)$  is a non-zero constant in  $C(K)$ . By Proposition 5, there exist a logarithmic extension  $L$  and an element  $z \in L$  such that  $\partial^n(z) = 1$ . Since  $\partial^n(w) = 0$ , Lemma 8 implies that  $w = \sum_{k=0}^{n-1} c_k \partial^k(\partial(z))$ , which leads to  $u = \partial\left(v - \sum_{k=0}^{n-1} c_k \partial^k(w)\right)$ . Thus  $u$  admits an antiderivative. ☺

We have the slightly stronger statement:

**Theorem 4** *Let  $(K, \partial)$  be an antiderivable differential field, and  $u \in K$ . Either  $u$  admits an antiderivative in  $K$ , or it admits an antiderivative in a logarithmic extension  $L$  such that  $C(L) = C(K)L^p$ .*

**Example 3** *We look for the characteristic  $p$  analogue of the antiderivative of  $\exp(\exp(x))$ .*

*Consider the differential field  $K = (\mathbb{F}_p(E, F), \partial)$ , where  $\partial(E) = E$  and  $\partial(F) = EF$ . From the obvious equation  $\partial^p(E) - \partial(E) = 0$  and Lemma 5, we obtain the equation  $\partial^p(F) - \partial(F) = E^p F$ . We conclude that  $\frac{\partial^{p-1}(F) - F}{E^p}$  is an antiderivative of  $F$ .*


**Example 4** *Consider the differential field  $K = (\mathbb{F}_p(X), \partial_K)$ , where  $\partial_K(X) = 1$ , and we look for an antiderivative of  $X^{p-1}$ . The differential field  $L = (\mathbb{F}_p(X, Y), \partial_L)$ , where  $\partial_L(X) = 1$  and  $\partial_L(Y) = 1/X$ , is a logarithmic extension of  $K$  and we see that  $\partial_L(Y X^p) = X^{p-1}$ .*

**Theorem 5** *Let  $(L, \partial)$  be an elementary extension of  $(\mathbb{F}_p(X), \partial)$  where  $\partial$  is the standard derivation. Every element  $u \in L$  admits an antiderivative in some elementary differential extension of  $(\mathbb{F}_p(X), \partial)$ .*




## 6 Linear differential equations

**Theorem 6** *Let  $(K, \partial)$  be an antiderivable differential field and  $Q \in C(K)[X]$ . The linear differential equation  $Q(\partial)(y) = 0$  admits a solution in some elementary extension of  $K$ .*

 The proof extends Euler's method of looking for a solution of the form  $\exp(\alpha x)$  for equations with inseparable characteristic polynomial.


Assuming  $Q \neq 0$ , we write  $Q = P(X^{p^e})$  with  $e$  as large as possible, so that  $P' \neq 0$ . Since  $K$  is antiderivable, there exists  $u$  in some elementary extension  $L_1$  of  $K$  such that  $\partial_{L_1}^{p^e}(u) = 1$ . We consider a separable extension  $L_2 = L_1(\alpha)$  of  $L_1$  such that  $\partial(\alpha) = 0$ , and the exponential extension  $L_3/L_2$  generated by  $E$  such that  $\partial_{L_3}(E) = \alpha \partial_{L_2}(u)E$ . By again applying Carlitz's formula we obtain

$$\partial^{p^e}(E) = \left( \sum_{i=0}^e \alpha^{p^{e-i}} \partial^{p^i}(u)^{p^{e-i}} \right) E . \quad (10)$$

The polynomial  $A(X) = \sum_{i=0}^e X^{p^{e-i}} \partial^{p^i}(u)^{p^{e-i}}$  is equal to  $\sum_{i=0}^{e-1} X^{p^{e-i}} \partial^{p^i}(u)^{p^{e-i}} + X$  so belongs to  $C(L_1)[X]$ . Furthermore,  $A' = 1$  and  $\partial^{p^e}(E) = A(\alpha)E$ . Thus  $Q(\partial)(E) = P(A(\alpha))E$ . Setting  $R = P(A(X))$  we have that  $R' = P'(A(X))$  is non-zero since  $P'$  is non-zero. Thus  $R$  admits a root  $\alpha$  in some separable extension  $L_2$  of  $L_1$ , so it follows that  $Q(\partial)(E) = 0$ . Note that the degree of  $R$  is equal to the degree of  $Q$ . 

To conclude we give a partial proof of the result below:


**Theorem 7** *Let  $(K, \partial)$  be an antiderivable differential field and  $P \in K[X]$ . The linear differential equation  $P(\partial)(y) = 0$  admits a solution in some elementary extension of  $K$ .*

 Without loss of generality, we can assume  $P$  to be monic, and we write

$$P = \sum_{i=0}^n p_i X^i .$$

Let  $L$  be the differential field  $(K(Y_0, \dots, Y_{n-1}), \partial)$  where  $\partial(Y_i) = Y_{i+1}$  if  $i < n-1$  and  $\partial(Y_n) = -\sum_{i=0}^{n-1} p_i Y_i$ . We see that  $P(\partial)(Y) = 0$ .

Since  $Y$  satisfies a differential equation with coefficients in  $K$ , by Theorem 2, it satisfies a linear differential equation  $Q(\partial)(Y) = 0$  with  $Q \in C(K)[X]$ .

By using the Euclidean division in the ring of differential operators  $K[X, \delta]$  it is possible to construct a differential polynomial  $R \in K[X, \delta]$  such that if  $Q(\partial)(f) = 0$ , then  $P(\partial)(R(f, \partial)) = 0$ . By the previous theorem, the equation  $Q(\partial)(f) = 0$  admits a solution in some elementary extension of  $K$ . Assuming the solution is sufficiently generic, the element  $R(f, \partial)$  will be a non zero-solution to  $P(\partial)(y) = 0$ . 

## References

- [A] G. B. Airy, *On the intensity of light in the neighbourhood of a caustic*, Transactions of the Cambridge Philosophical Society (University Press) textbf6 (1838), 379–402.
- [C] L. Carlitz, *Some congruences for the Bell polynomials* Pacific J. of Math. **11** No. 4 (1961), 1215–1222.

- [J] N. Jacobson, *Basic Algebra I*, Freeman, San Francisco (1974).
- [L] J. Liouville, *Mémoire sur la classification des transcendentes et sur l'impossibilité d'exprimer les racines de certaines équations en fonction finie explicite des coefficients*, Journal de mathématiques pures et appliquées **2** (1837), 56–105 and **3** (1838), 523–547.
- [Ri] R. H. Risch, *The problem of integration in finite terms*. Trans. Amer. Math. Soc. **139** 1969, 167–189.
- [Ro] M. Rosenlicht, *On Liouville's theory of elementary functions* Pacific J. of Math. **65** (1976), no. 2, 485–492.

Bill Allombert

CNRS, Institut de Mathématiques de Bordeaux, UMR 5251,

Université de Bordeaux, 351 cours de la Libération, F-33405 Talence Cedex, France

email: bill.allombert@math.u-bordeaux.fr